Wat zijn de vijf pilaren van Deliverability?

Deployteq - Suzanne Martens - 2023-11-30 - Reacties (0) - Deliverability

Om een mail goed aan te laten komen is het belangrijk om de 5 pilaren van deliverability goed te begrijpen:

1. Strategie
2. Databasekwaliteit
3. Content
4. Authenticatie
5. IP-reputatie

Strategie

Maildruk, relevantie, call to action. Zorg ervoor dat je op deze drie onderwerpen een strategie klaar hebt liggen die past bij je eigen praktijk.

De ideale maildruk bestaat niet. Het aantal e-mails dat gewenst is, is heel brancheafhankelijk. Een website met dagaanbiedingen kan iedere dag een e-mail versturen, die goed geopend wordt. Wanneer een verzekeraar zijn hele bestand iedere dag mailt, dan is de kans groot dat dit niet gewaardeerd wordt. Onderzoek dus welke maildruk past bij je branche en blijf hier kritisch op.

> **Relevantie**: wellicht een open deur, maar het is enorm belangrijk om mails te versturen die relevant zijn voor de ontvanger. Er kan meer activiteit gemeten worden in relevante e-mails (opens, kliks) wat zorgt voor een betere reputatie.

Voorbeeld: een slijterij verstuurt traditioneel gezien veel informatie over wijnen. Maar: er zijn klanten die niet van deze wijn houden, wel van whiskey. Dan is het van belang dat je bij klanten die nooit wijn drinken, zorgt voor voldoende andere relevante content. Over whiskey dus!

Als die e-mail eenmaal geopend is, dan is het zaak om een goede call to action aan te bieden. Is duidelijk wat je e-mail beoogt te bereiken? Motiveren de linkjes om erop te klikken? Een goede call to action zorgt voor meer interactie in je e-mails, wat ook weer goed is voor je reputatie.

Databasekwaliteit

Als de kwaliteit van je klantendatabase niet op orde is dan heeft dit direct invloed op je reputatie bij de mailboxprovider. De kwaliteit is op twee manieren te kwalificeren:

- Kloppen de e-mailadresen?
- Welke activiteit vertonen de e-mailadressen?

Een bekend spreekwoord in statistische analyse is: ‘garbage in = garbage out’. Dit geldt ook voor je database. Het is daarom van belang om de de kans op incorrecte e-mailadressen (en daardoor bounces) in je base te minimaliseren:

- Importeer geen oude databestanden. Zeker nooit bestanden van > 1 jaar oud! Bij twijfel: neem contact met ons op.
- Zorg voor correcte invoer. Merk je dat er veel bounces optreden naar aanleiding van nieuwe inschrijvingen? Dan kun je bijvoorbeeld het volgende doen:
    - E-mailadres dubbel in laten voeren op het aanmeldformulier. Alleen bij overeenkomst opnemen in je database.
    - Laat een tool als BriteVerify of Kickbox de kwaliteit van het ingevoerde e-mailadres beoordelen voordat je het mailt.
- Werk met een dubbele opt-in: pas nadat de inschrijving bevestigd is door middel van een klik op een link in een bevestigingsmail is het mogelijk om het adres te benaderen. Wellicht hou je daarmee per saldo minder e-mailadressen over, maar bijkomende voordelen:
    - De mensen die de bevestigingslink aangeklikt hebben, hebben daarmee extra commitment afgegeven en blijken in de praktijk vaak actiever te zijn.
    - Het klikken op de link levert meteen een interactie op die door de mailbox provider geregistreerd wordt. Goed voor je engagement score! (zie hieronder)
    - Een eventuele bounce wordt geregistreerd op een één op één bericht i.p.v. als onderdeel van je eerstvolgende grote verzending. Wanneer je op een grotere verzending een te hoog bouncepercentage genereert, loopt het goed afleveren van de hele verzending gevaar.
- Het gebruik van dubbele opt-ins beschermt je ook tegen spamtraps. Vergelijk een spamtrap met een landmijn. Die kun je niet zien als je over een stuk gras loopt, maar als je hem raakt zit je direct in de problemen. Spamtraps zijn e-mailadressen die eerder door een gebruiker afgesloten zijn, maar na een tijdje weer heropend zijn door de mailbox provider. Als jouw berichten in een spamtrap belanden betekent dit dat de databasekwaliteit niet op orde is. Immers: er is al diverse keren een bouncestatus afgegeven voor dit mailadres en toch blijf je het mailen. Ook kan het

niet zo zijn dat dit recentelijk in je database terecht gekomen is. Wanneer je een spamtrap mailt is de kans op een blacklisting groot en dit wil je ten alle tijden voorkomen – want dan komen je mails ook niet meer aan bij de bestaande mailadressen.

- Mail frequent en houd de databasekwaliteit zo op peil.

Tweede aspect is de activiteit van je e-mailadressen, ook wel engagement genoemd. Hoe meer opens/clicks er zijn na het sturen van de e-mail, hoe beter. Wanneer een mailbox provider ziet dat er weinig activiteit is, kunnen ze besluiten om je e-mails niet meer in de inbox af te leveren.

Je kunt dit verbeteren door:

- Campagnes in te richten die inactieve e-mailadressen proberen te reactiveren en wanneer dat niet lukt: veel minder tot niet meer te mailen. Dit kun je eenmalig doen om de base flink op te ruimen, maar het mooiste is om dit doorlopend in te richten.
- Te letten op het versturen van relevante content: geen bulk e-mails meer maar gepersonaliseerde content! Begin klein, de eerste stap is zo gezet.

Binnen Deployteq kun je met behulp van de engagement scoring module (standaard actief) selecties maken op basis van activiteit van je database.

Content

Houd rekening met de volgende eisen aan de inhoud van je e-mail, zodat deze niet door de mailboxprovider geblokkeerd wordt:

- Zorg dat de e-mail niet te zwaar is. Wij adviseren maximaal 101 kB code, met de afbeeldingen erbij tot een maximale totale berichtgrootte van 250 kB;
- Stuur altijd een tekstversie mee, met daarin gedeeltelijk dezelfde inhoud. Denk aan de naam van je organisatie, titel van de e-mail, het bovenste artikel en de informatie en linkjes uit de footer. Dus ook een afmeldlink! Voor het vervolg van de mail kun je doorverwijzen naar de online versie.
- Neem je fysieke adres op in de footer van je template;
- Plaats de uitschrijflink ook in de header van je template, wat voorkomt dat mensen zich afmelden door middel van een spam complaint;
- Gebruik geen woorden als ‘gratis’ en ‘win’ en vermijd zoveel mogelijk het gebruik van hoofdletters;
- Maak gebruik van een goede subjectline. Zie het als lingerie: het moet er mooi uitzien en het geeft je een inkijkje wat erachter zit, zonder direct teveel weg te geven. Je wordt verleid om over te gaan tot openen! Vermijd ook hier woorden zoals ‘gratis’ en ‘win’ en laat het zo goed mogelijk passen bij de ontvanger. Deze bepaalt

uiteindelijk of het voldoende interessant is om open te maken; Onze ingebouwde subject line optimizer helpt je graag verder!

- Last but definitely not least: check altijd eerst je content via de gratis dienst EmailAnalyzer: https://analyze.email/. Als je e-mail lager scoort dan een 9, blijf sleutelen aan de inhoud en test het nog een keer. De tool geeft o.b.v. 5 punten aan wat er beter kan aan de content.

Authenticatie

Het gaat er uiteindelijk om dat je e-mail zo legitiem en betrouwbaar mogelijk eruitziet. Je identificeert jezelf als een goede en betrouwbare afzender (denk terug aan het voorbeeld van het postpakket). De authenticatie bestaat uit de volgende technische onderdelen: SPF, DKIM & DMARC.

Dit zijn toepassingen die het beveiligen van mailverkeer overzichtelijker en makkelijker maken. Als deze niet goed zijn ingesteld, kan dit gevolgen hebben voor je reputatie.

- Sender Policy Framework (SPF): Dit is een TXT-record dat aangemaakt wordt in de nameserver configuratie van het domein. Het bevestigt simpelweg dat je toestemming hebt om te mailen namens @domeinnaam.nl;

- DKIM: Dit omhelst de koppeling tussen de mailservers en de DNS (Domain Name System) die hiermee de echtheid van je e-mails kan bevestigen;

- DMARC: Dit is een maatregel om phishing te voorkomen, het omvat de combinatie van een goed ingestelde SPF en DKIM. DMARC controleert of het ‘header from’ veld met de SPF record in de e-mail overeenkomt, inclusief DKIM handtekening. Als de e-mail door deze controles heen is gekomen wordt deze bij de ontvanger afgeleverd.

IP-reputatie

Of je e-mail terecht komt in de inbox, spamfolder of in zijn geheel wordt geblokkeerd heeft voor een groot deel te maken met je IP-reputatie. Dit noemen we ook wel de ‘Sender Score’, het is de beoordeling van je mailserver op een schaal van 0-100. Deze score wordt gegenereerd door een algoritme dat naar de statistieken van de afgelopen 30 dagen kijkt uit diverse e-mailclients en de ontvangers. De onderstaande factoren zijn hierbij van belang:

- Aantal personen dat je e-mail opent;
- Aantal reacties op de e-mail;
- Het aantal keer dat de e-mail als spam is gemarkeerd;
- Aantal keer dat de e-mail is verplaatst naar een andere map;

- Aantal keer dat de e-mail is doorgestuurd naar een ander;
- Het aantal keer dat de e-mail wordt verwijderd voordat deze geopend is.

De IP-reputatie hoog houden is onze core business, hier hoef je als klant je dus geen zorgen over te maken. Wij monitoren dit actief en nemen gepaste actie mits noodzakelijk.